Disruption Tolerant Networking (DTN) for Aviation Use

Leigh Torgerson

Space Communications Networking Architect

Jet Propulsion Laboratory

California Institute of Technology

ltorgerson@jpl.nasa.gov

818-393-0695

Introduction

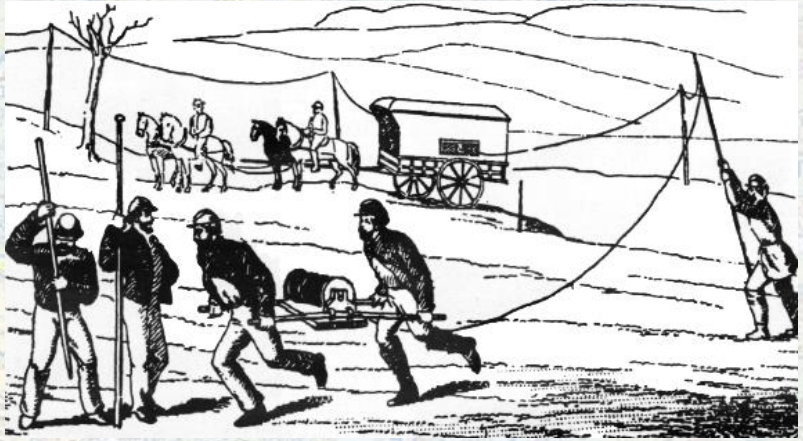
- This slide package was adapted from material used to brief Department of Defense interests, but the applicability to commercial aviation should be easily inferred.
- Slides were taken from several public presentations by JPL as well as slides by Jason Soloff from JSC as presented at a IEEE Conference in December 2015.
- Slides should be viewed in presentation mode since some are animated.

- The first thing to point out is that communications have always been based on end-to-end techniques, where there is a continuous path from sender to receiver. Subsequent slides explain why this is difficult, and how DTN is a valuable solution to the inevitable loss of links along the way.

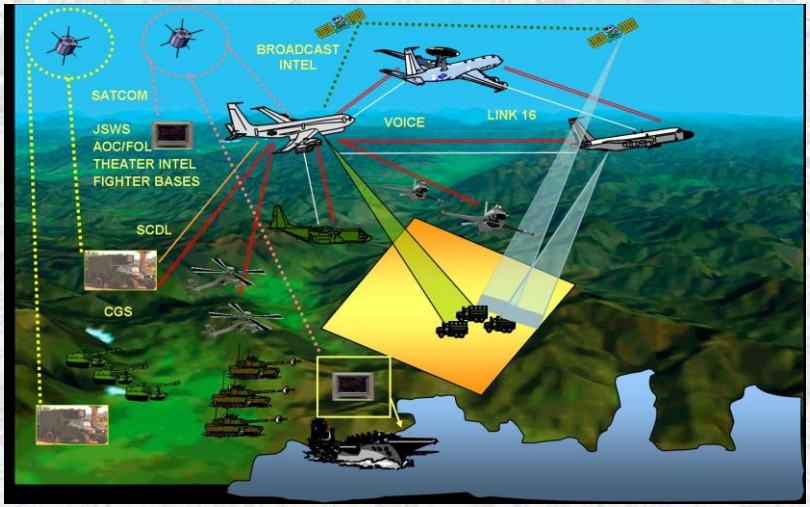
(There are additional comments in the note section below many of the slides)

160 Years of Military Comm Evolution

From telegraph



to “Netcentric Warfare”



What's Wrong With This Picture?

The assumption cannot always be made that the comm path is connected end-to-end

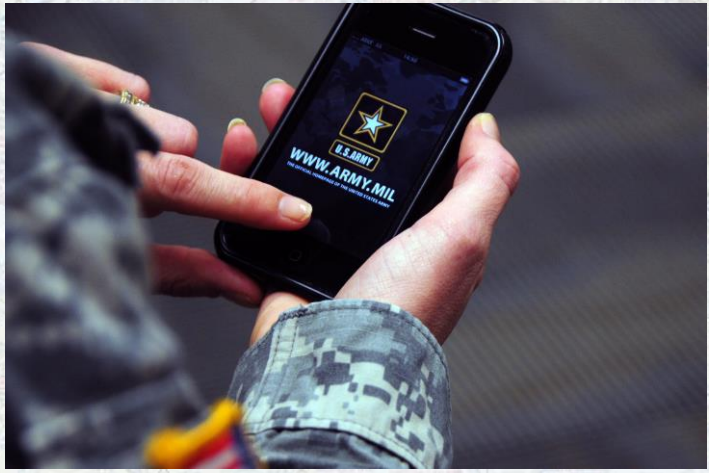
What Has DoD Done to Improve Comm?
- the focus has been on robust connectivity -

Complex computer systems

Expensive antenna systems

Field satcom

JTRS



Now even cell phones at the tactical edge

4G Comm defeated by 4G Warfare….

But even the best systems are subject to disruption!

Cell phone edge systems are easy to disrupt and are frequently targeted in war zones

https://techcrunch.com/2008/03/27/taliban-attacking-cell-towers-in-afghanistan/

http://www.cbc.ca/news/world/third-attack-on-cellphone-tower-in-afghanistan-1.774276

Why Disruption Tolerant Networking is Needed

"Netcentric" operations relies on the end-to-end model used by terrestrial networking and telephony

But this is problematic:

- E2E is hard to maintain
- susceptible to weather, link range/power availability, and many unpredictable events
- Many links are easy to defeat (think terrorist in the context of civil aviation) –
  - Ka Band can be stopped with a good rain storm
  - Secure 802.11 WiFi is easy to jam
  - Frustrated users may attempt insecure workarounds
- Urban adversaries can disrupt YOUR network while freely using THEIR network

In any case, even in the absence of adversarial network disruption, network outages are frequent, and reliable end-to-end communications to the edge nodes in long range situations is difficult, costly and ultimately unlikely.

The moral of the story is that end-to-end networking is hard in many environments

Why is this an issue? Let's take a quick look at how standard internet protocols work:

Five Key Assumptions of the Internet Protocols

1. ***Networks are Richly Connected***

   IP Networks assume that there are many link paths between routers and that those links are consistent with high availability.

   – "If I can reach you, you can reach me" *(reachability is symmetric)*

   – "If I can reach you, and you can reach her, I can reach her." *(reachability is transitive)*

2. ***Networks have Short Delay***

   IP networks assume that the time to propagate a packet across an IP network is small – on the order of ms to second

3. ***Data Links are Symmetric and Bidirectional***

   IP networks assume that forward and return bandwidths are approximately the same and that forward and return connections will only exist in pairs.

4. ***Links have Low Error Rates***

   The likelihood of a packet not making it from end to end due to errors in transmission is fairly low (typically << 1e-8)

5. ***Network Nodes are Trustworthy***

   IP assumes that if a node (router or computer/device) is ON the network it is trustworthy. Additional protocols (eg. IPSEC) provide security enhancements, but core protocols assume a trusted environment.

Conclusion:
Standard Internet Protocols Do Not Work Well in Many Environments!

- In networks that are characterized by frequent link drops, prone to weather-related dropouts, dependent upon satcom relays that may not always be available, the terrestrial Internet Protocols do not work very well.

1. ***Networks at the edge of the rich connectivity we described are poorly connected***
2. ***Edge networks have periods of being disconnected, which looks like delay to an internet computer.***
3. ***Data Links are often asymmetric and unidirectional***
4. ***RF Links often have high error rates, especially when aircraft maneuver***
5. ***Network Nodes may be trustworthy, but RF links make hacking potential skyrocket***

- DTN was developed to work around these difficulties of end-to-end connectivity with mobile or airborne elements!

Delay-Tolerant Networking (DTN)

- Internet depends on end-to-end connectivity; DTN uses "Pony Express" store and forward connectivity model
- An overlay network.
  - DTN "bundle protocol" (BP) is to IP as IP is to Ethernet.
  - A TCP connection within an IP-based network may be one "link" of a DTN end-to-end data path; a deep-space R/F transmission may be another.
- Reliability is achieved by retransmission between relay points within the network, not end-to-end retransmission.
- Route computation may have temporal as well as topological elements, e.g., a schedule of planned contacts.
- Forwarding at router is automatic but not necessarily immediate: store-and-forward rather than "bent pipe".
- DOS attacks contained: reciprocal inter-node suspicion.

Traditional Internet Transfers vs. DTN Transfers

In the Internet:

- Each received packet is forwarded immediately if possible, deleted if immediate forwarding is not possible.
- Next-hop destination is computed based on known current network topology.

In DTN:

- Each received packet is forwarded immediately if possible, stored for future transmission if forwarding is not currently possible but is expected to be possible in the future.
- Next-hop destination is computed based on expectations of future network topology.

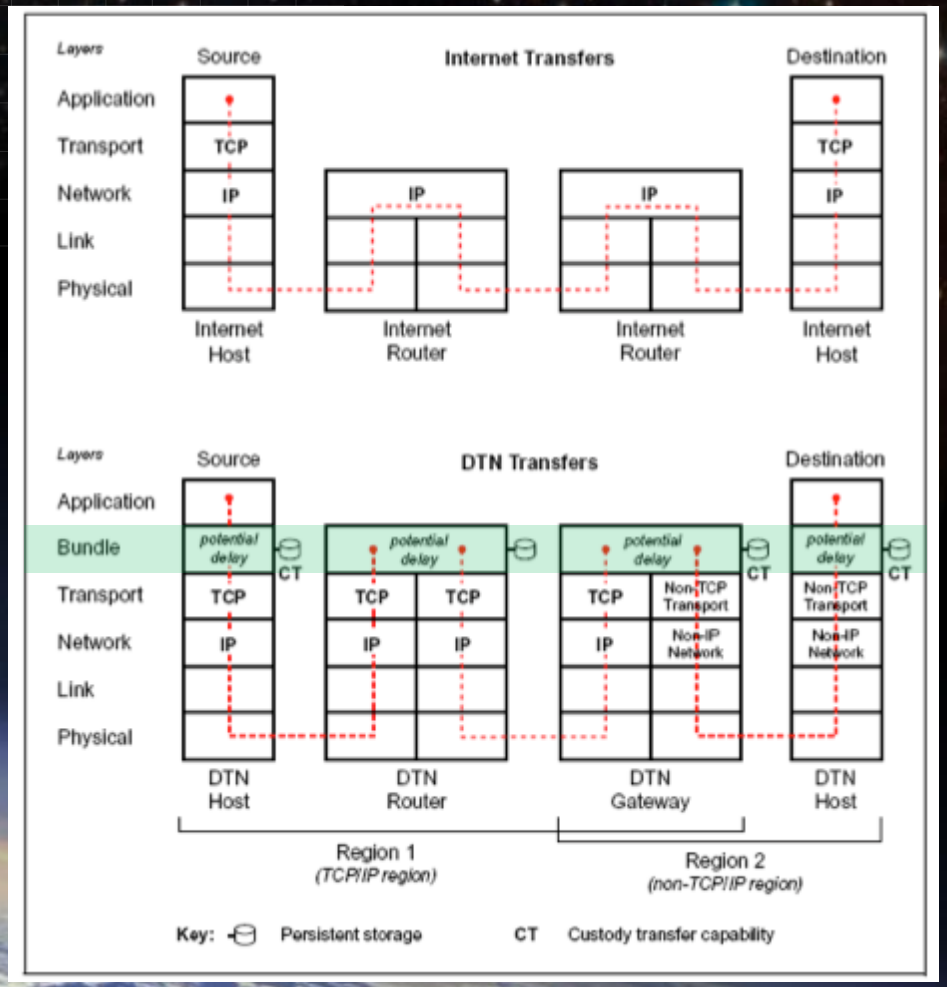
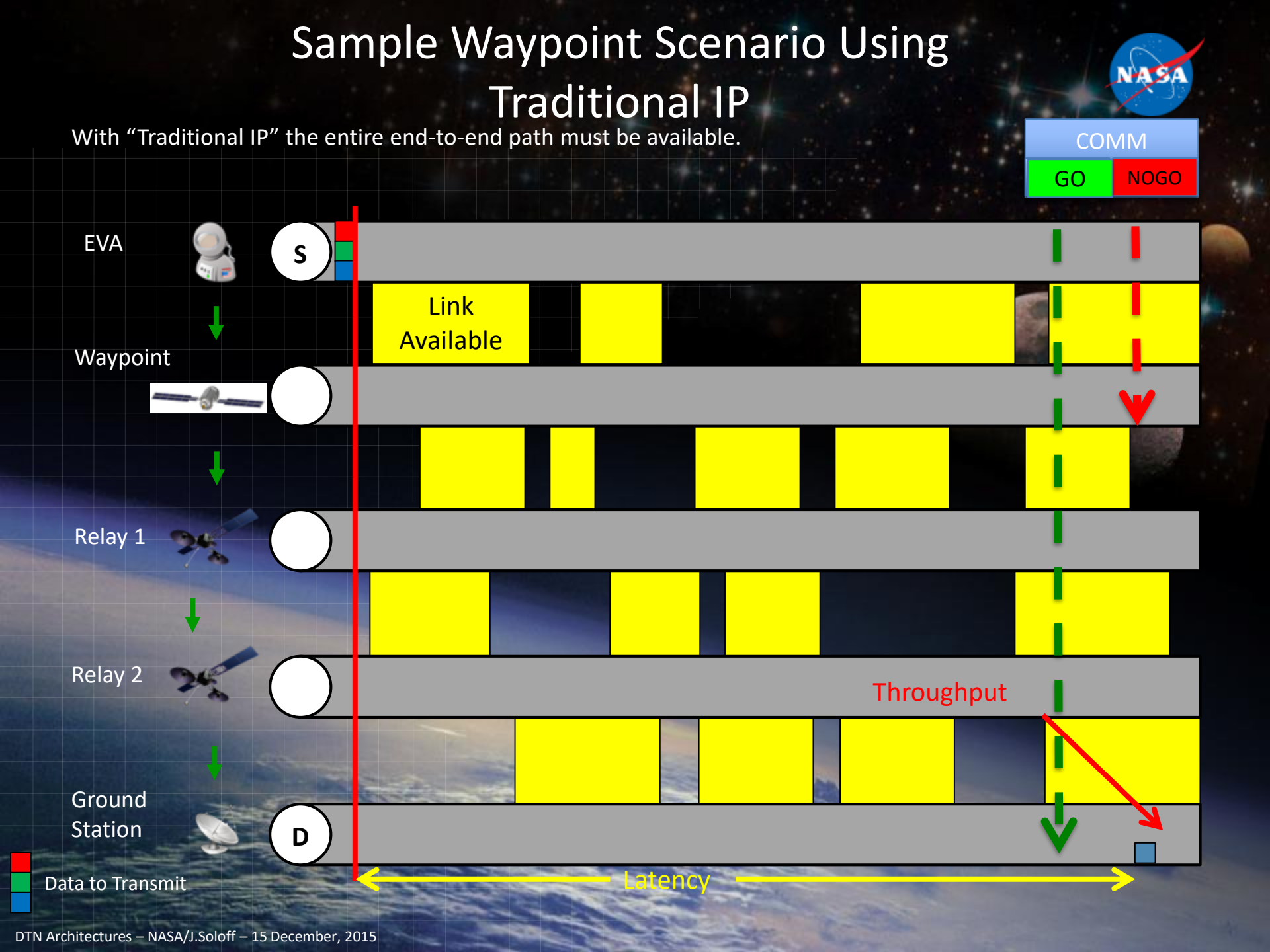


Figure taken from "Delay and Disruption Tolerant Networks: A Primer", F. Warthman
http://ipnsig.org/wp-content/uploads/2012/07/DTN_Primer_v1.02.pdf

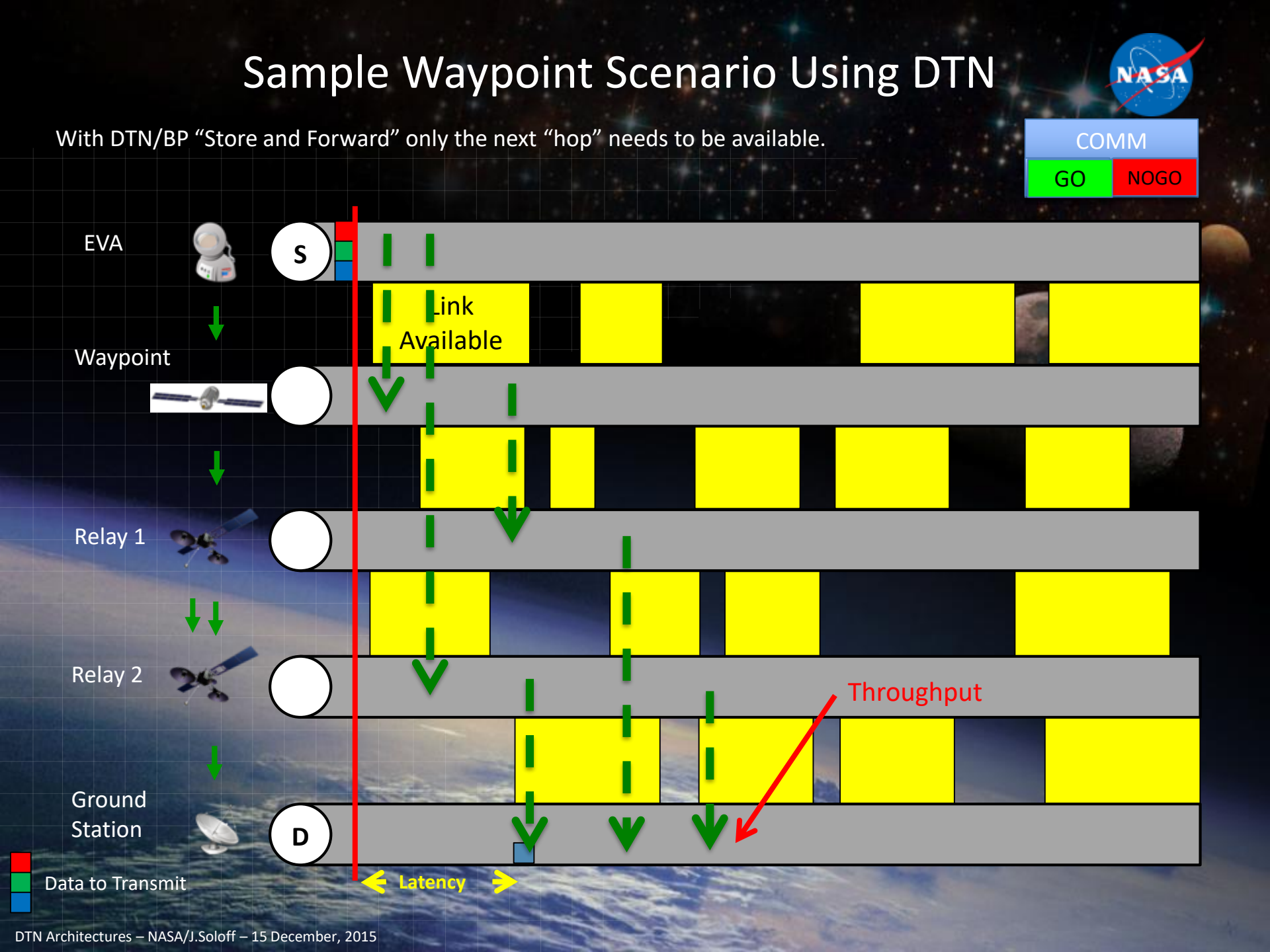
Sample Waypoint Scenario Using Traditional IP

With "Traditional IP" the entire end-to-end path must be available.



Sample Waypoint Scenario Using DTN

With DTN/BP “Store and Forward” only the next “hop” needs to be available.

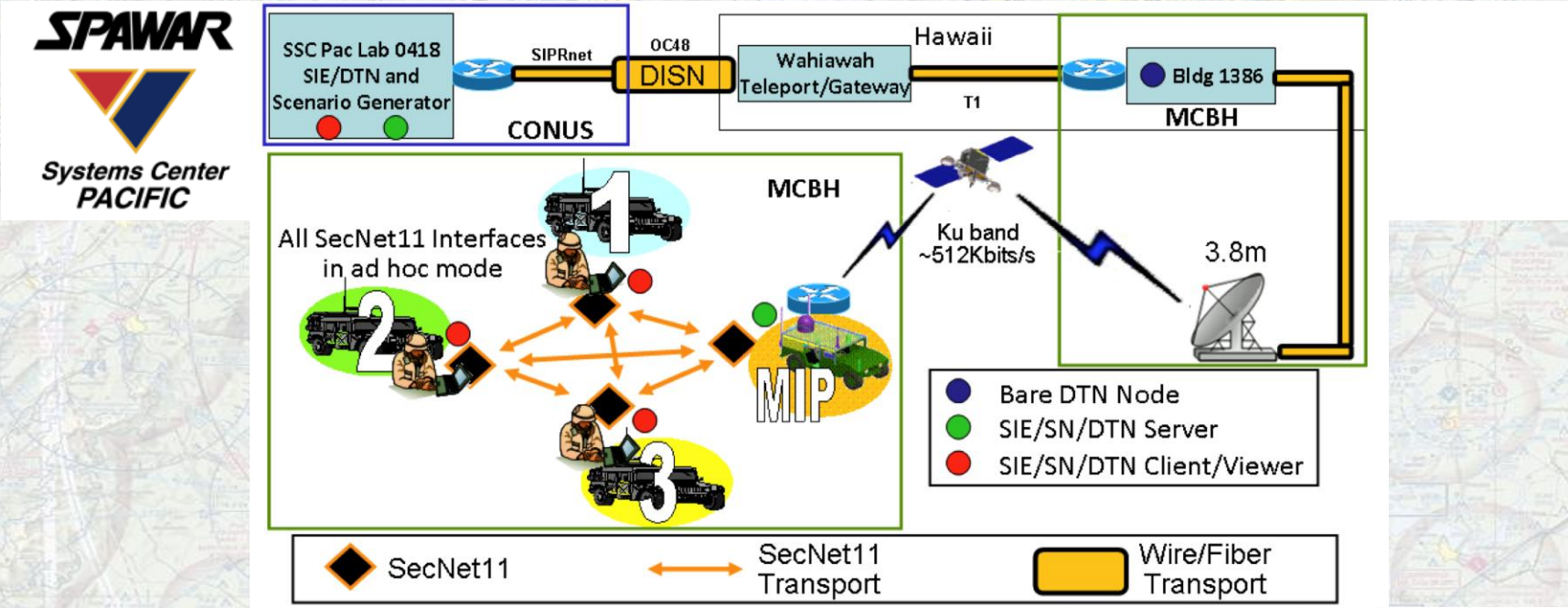


- One use case example; (with Humvees instead of aircraft, but the principle is the same!)

DARPA DTN Program tests with USMC in 2010

Field Tests – USMC Base Hawaii

- Field tests were conducted January 18-29 at MCBH



From SPAWAR SIEDTN Test Plan v1.1, January 13, 2010

Test Summary

- 1000 position/velocity updates per minute on aircraft and land force contacts sent over satellite from San Diego to MCBH to a communications vehicle –
  - DTN used to store and forward data when satcom channel was disrupted

- Communications vehicle relayed contact data to 3 mobile units in the field using 802.11, while vehicles maneuvered and simulated various tactical scenarios
  - Tests with and without DTN were conducted for several weeks
  - Non-DTN legacy systems received 1/3 or less of the contact data
  - DTN systems allowed 100% of the data to be received by tactical mobile units

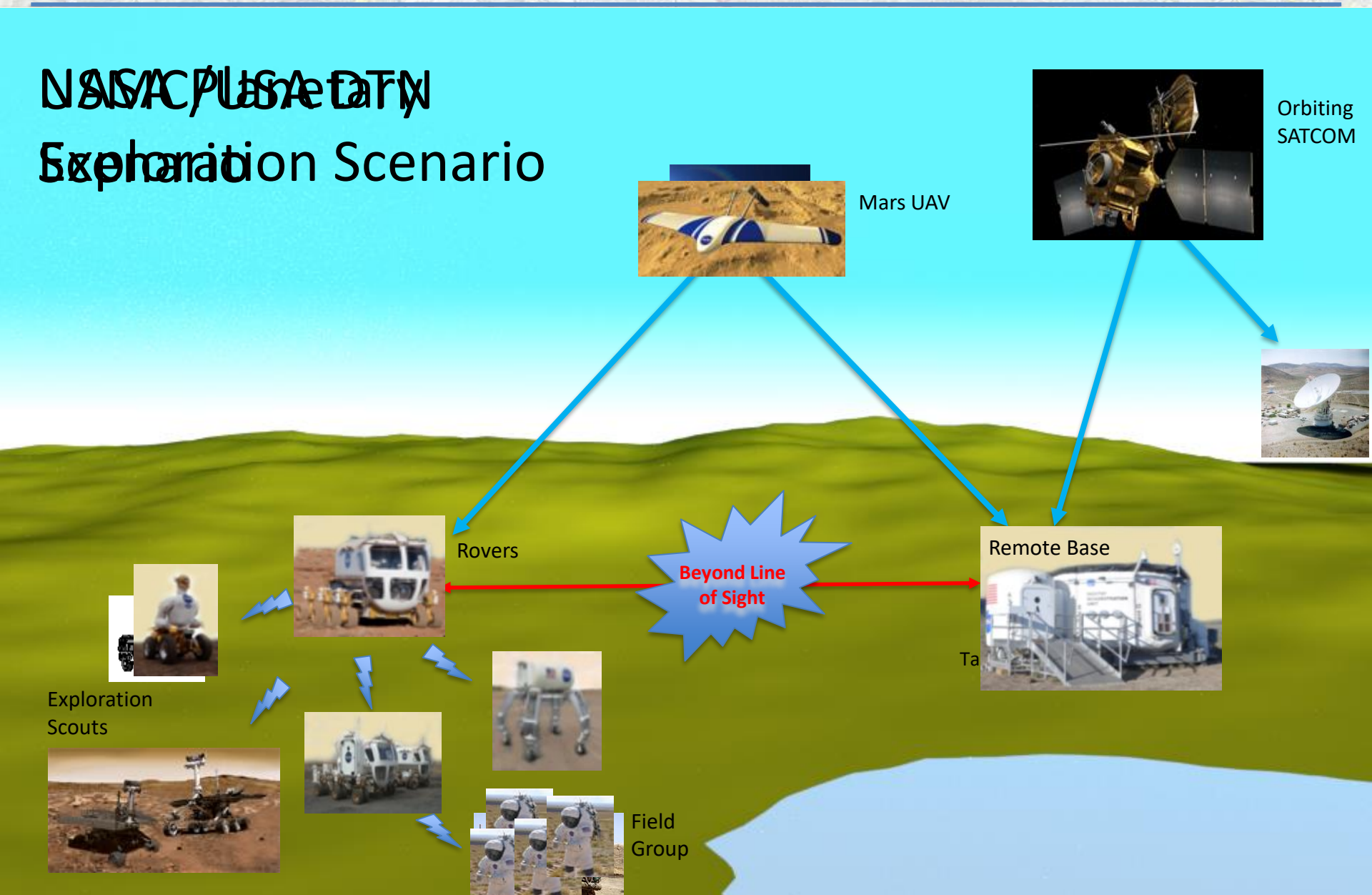
DTN delivers the data!

Over 100 of test runs of 20-30 minutes duration conducted in both Hawaii and in Pasadena

DTN consistently demonstrated successful data delivery to disconnected tactical nodes that were unreachable using standard internet protocols

One Architecture, Many Missions

Exploration Scenario



A More Capable Architecture – Disruption Tolerant Networking

DTN is… an internetworking protocol suite suitable for disrupted, mobile, airborne, near-Earth and deep-space communications:

- An internetworking layer that functions efficiently in environments with time-disjoint and/or simplex links
- A reliable data link layer that improves efficiency of end-to-end delivery by leveraging local link information and tighter local control loops
- Disruption Tolerant Routing services that can take advantage of scheduled and expected future connectivity in addition to current connectivity and that can interoperate with or without a terrestrial routing infrastructure
- Quality of Service mechanisms to provide user control over the order in which traffic is served by the overlay internetworking layer and is independent of the underlying network segments
- Security features that protect the infrastructure from unauthorized traffic and provide standard end-to-end security capabilities (e.g. integrity, confidentiality) and 'over-the-air' key management
- A network management system to configure, monitor, and provide accounting for traffic passing through the system
- International standards (IETF & CCSDS)

DTN for Flight Ops Data Communications Features and Advantages

- End-to-End Connectivity NOT NEEDED if DTN is used
- Automatic **relay** operations.
  - Retain data until outbound link is available.
  - Then transmit until link is no longer available.
- Fine-grained **routing**: automatic selection of (possibly parallel) links to transmit over, based on the final destination of the data.
- Automatic selection of data to transmit, based on mission-specified **priority**.
- Automatic **retransmission** of lost or corrupted data.
- Automatic **aggregation** of data into blocks, to limit return traffic (acknowledgments).
- **Custodial forwarding**, for early release of retransmission buffer space.
- Automatic **congestion control**, based on rate management.
- Automatic **data aging and purging** based on bundle's "time to live".
- Optional status reports for detailed **tracing and data accounting**.
- Support for **file transfer**, **message exchange**, **multi-point delivery**.
- Support for **security**: end-to-end encryption & cryptographic integrity.

Current DTN Status

- ISO CCSDS Standard now, is being standardized in IETF
- NASA is adopting DTN for new missions, infusing into DSN and NEN systems
- NASA plans on using it in optical comm systems
- DTN now on the ISS on both the payload LAN and the OPS LAN
- 5 NASA centers are working on DTN systems
  - with NASA baseline implementation being the JPL space-qualified ION DTN implementation.
  - Open Source version available at http://ion-dtn.sourceforge.com
- NASA Armstrong (Dryden) / JPL have collaborated on designs for a flight test DTN network for National Flight Test ranges
- Security
  - BPsec under development; APL & LTS focus on NSA-approved techniques
  - Asymmetric key exchange and Delay-Tolerant Key Management protocol available
- Implementations
  - Light-weight; has run on cubesat microprocessors, cell phones, Linux, Windows and OS-X
- Applications
  - Some applications immediately work over a DTN;
  - Others require a paradigm shift (have to abandon the end-to-end model)

POTENTIAL USE CASES

IEEE WiSEE 2015 Conference Slides by Jason Soloff, NASA JSC

NASA High Altitude Research Program (WB-57)

- WB-57 provides scientists with high-altitude (>65k ft) access for payloads
  - Users include NASA, NSF, NPS, NOAA, Universities
- Payload / Mission communications currently provided by INMARSAT and /or ViaSat IP services – requires either accommodating outages due to IP or reliance on proprietary "IP enhancement protocols"
- Comms is often disrupted due to A/C maneuvering, obstruction, satellite handoff, etc.
- **NASA WB-57 Program working with AES DTN Project to implement ION DTN and a BP-based network architecture from flight to ground as a standard service to experimenters.**

- Host ION DTN on existing science comms. computer
- Enable both IP and BP traffic (per experimenter choice)
- Provide support (as a program) for TREK science console

DHS / USCG / CBP

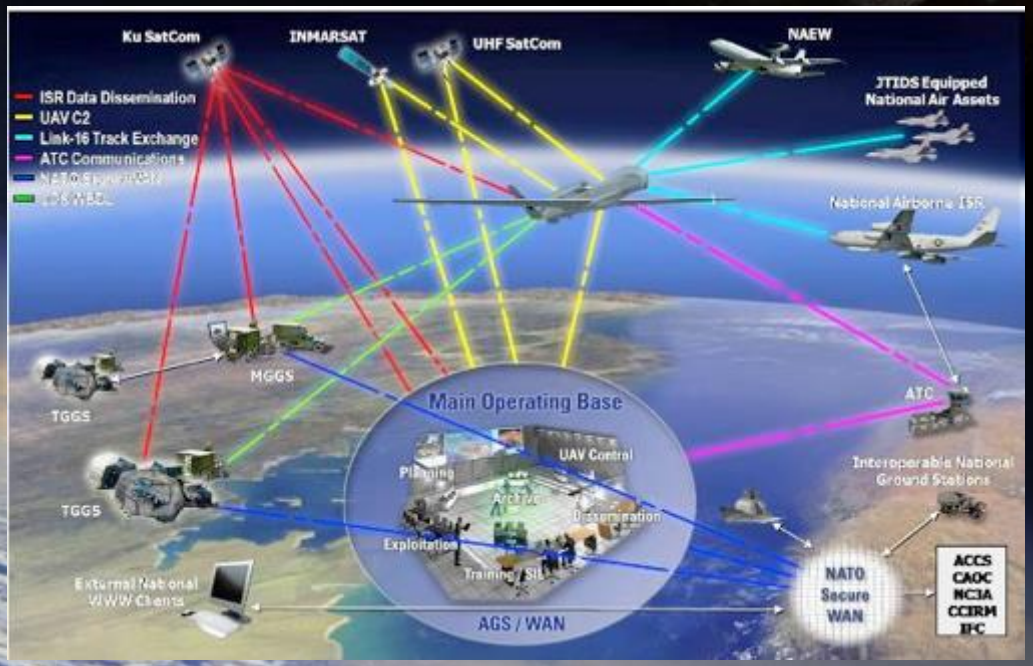
- Maritime AIS
- Cargo / Person Tracking
- Vessel Identification
- Harbor security
- Border security
  - SensorWeb monitoring
  - UAV/UAS comm “mules”
- Customs processing
  - “Gold Lanes”
  - Traffic monitoring

Arctic / Combat Search & Rescue

- Integrated communications is a severe challenge
  - Victims may not be able to remain exposed for communication… contact is expected to be spotty
  - (CSAR) Comms on a schedule may not be possible / practical
  - Recovery not necessarily immediate
- DTN useful for comm relay, message store & forward, opportunistic comms

UAV / UUV / C3 Communications

- Civil / Commercial “UAV” Operation
- Earth Science
- Maritime Domain Awareness
- Joint Information Networks



Questions?

BACKUP SLIDES

Additional DTN Services (1 of 2)

- Bundle Streaming Service (BSS)
  - A framework that supports the delivery of streaming data in DTN bundles, by placing priority on “real-time” data and backfilling any stored data when link bandwidth permits.
- Delay-Tolerant Payload Conditioning (DTPC)
  - A DTN service that guarantees in-order delivery and suppression of duplicate data.
- Aggregate Custody Signals (ACS)
  - Makes more efficient use of narrow command path by compressing many custody signals into one.
- Compressed Bundle Header Encoding (CBHE)
  - A convention by which BP convergence-layer adapters may represent endpoint identifiers in a compressed form within the primary blocks of bundles, which aids in improving efficiency on space links.

Additional DTN Services (2/2)

- Delay-Tolerant Key Authority (DTKA)
  - A key exchange framework that is based on distributed KA nodes that provide bulletin services to DTN clients
- DTN IP Neighbor Discovery (IPND)
  - IPND is a method for otherwise oblivious nodes to learn of the existence, availability, and addresses of other DTN participants
    - IPND sends and listens for small IP UDP announcement beacons that are addressed to an IP unicast, multicast, or broadcast address to discover specified remote neighbors, or unspecified local neighbors in the network topology
- Asynchronous Management Protocol (AMP)
  - AMP provides monitoring and configuration services between managing devices (Managers) and managed devices (Agents), some of which may operate on the far side of high-delay or high-disruption links.
- Streamlined Bundle Security Protocol (SBSP)
  - SBSP is an improved security specification to the previous RFC 6257 (BSP) that decouples routing/security functions, minimizes the number of security blocks and operations, adds common block processing and order, and simplifies rules for fragmentation. Will be standardized by IETF as BPsec.

DTN Implementations

- Interplanetary Overlay Network (ION):
  - http://sourceforge.net/projects/ion-dtn
  - NASA's primary DTN implementation (developed by JPL)
  - Includes implementations of BP and LTP as well as implementations of CFDP, BSS and AMS
  - Supported by multiple Operating Systems

- DTN2:
  - http://sourceforge.net/projects/dtn/
  - Includes an implementation of BP and BSP
  - Used at the MSFC HOSC

- Other DTN Implementations:
  - IBR-DTN: http://www.ibr.cs.tu-bs.de/trac/ibr-dtn
    - Available on the Google Play store and as an OpenWRT package
  - JDTN: http://sourceforge.net/projects/jdtn/
    - Java implementation developed by Cisco
  - Postellation: http://postellation.viagenie.ca/

Standardization

- Internet RFCs:
  - RFC 4838 – Delay Tolerant Networking Architecture
  - RFC 5050 – Bundle Protocol Specification
  - RFC 5326 – Licklider Transmission Protocol
  - RFC 6257 – Bundle Security Protocol Specification
  - RFC 6260 – Compressed Bundle Header Encoding (CBHE)

- CCSDS:
  - CCSDS 734.0-G-1 – Rationale, Scenarios, and Requirements for DTN in Space
  - CCSDS 730.1-G-1 – Solar System Internetworking Architecture Informational Report
  - CCSDS 734.2-B-1 (Approved 2015) – CCSDS Bundle Protocol Specification
  - CCSDS 734.1-B-1 (Approved 2015) – Licklider Transmission Protocol (LTP) for CCSDS
  - DTN Network Management Informational Report (Draft)